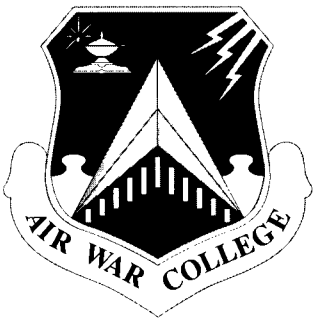
The Maxwell Papers

Seller Beware

US International Technology Transfer and Its Impact on National Security



Wayne M. Johnson
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 16

Air University

Joseph J. Redden, Lt Gen, Commander

Air War College

Lance L. Smith, Maj Gen, Commandant
Ronald J. Kurth, PhD, Dean
Lawrence E. Grinter, PhD, Series Editor
Grant T. Hammond, PhD, Essay Advisor

Air University Press

Robert B. Lane, Director
Richard Bailey, PhD, Content Editor
Carolyn J. McCormack, Copy Editor
Prepress Production: Linda C. Colson
Cover Design: Daniel Armstrong

Please send inquiries or comments to:
Editor
The Maxwell Papers
Air War College
Bldg 1401
Maxwell AFB AL 36112-6427
Tel: (334) 953-7074
Fax: (334) 953-4028
Internet: lagrinter@max1.au.af.mil

AIR WAR COLLEGE
AIR UNIVERSITY

Seller Beware

US International Technology Transfer and Its Impact on National Security

WAYNE M. JOHNSON
Lieutenant Colonel, USAF

Air War College
Maxwell Paper No. 16

MAXWELL AIR FORCE BASE, ALABAMA

December 1998

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any US government agency. Cleared for public release: distribution unlimited.

Foreword

As was the case during the cold war, the national military strategy of the United States relies on technologically superior forces to achieve our objectives when the armed forces are called on to protect the United States and its interests. However, as the military downsizes, preserving a technologically superior force while also maintaining a robust defense industrial base becomes more difficult. One means the United States uses to preserve the industrial base is to maintain demand by selling our military goods to other countries. While foreign military sales (FMS) alone will not keep the US industrial base viable, they have become more significant than in the days of larger US defense procurements. In 1996, for example, FMS exceeded $10 billion. Indeed, FMS can spell the difference between continued existence and bankruptcy for some of our defense contractors. The perceived need to sell overseas while safeguarding US advanced technologies appears to be a conflicting goal because of the technology transfer involved.

In this important study, Lt Col Wayne Johnson, USAF, argues that systematic tightening of interagency cooperation and better work on defining sensitive technology prohibitions are needed to maintain the US technological edge. He also maintains that the US government requires a new and disciplined export control process—not the current mosaic of rules, regulations, and perspectives that came out of the cold war, but a process that provides a revamped, systemic approach with consistent implementation. Colonel Johnson explores the problem of defining which technologies the United States is willing to transfer (military or dual-use) and the need to ensure that national security objectives do not take a backseat to economic expediency. To accomplish this end, he argues for better interagency cooperation as a first step leading to a more centralized, coordinated, and strategic view of technology transfer and how it impacts US national security.

Recent events concerning missile technology transfers point out the timeliness of this debate. These recommendations deserve to be read by a wide Department of Defense

audience, as the United States evaluates its policies to determine if short-term interests in selling high-technology arms to foreign countries can actually weaken rather than strengthen our national security.

LANCE L. SMITH
Major General, USAF
Commandant
Air War College

About the Author

Lt Col Wayne M. Johnson, USAF, is a command pilot with experience in B-52s, T-38s, and B-1s. His former assignments include a joint tour in the Strategic Target Plans Division at US Strategic Command, and he has been an acquisition program manager in the B-1 and F-16 Program Offices.

Colonel Johnson is a 1996 graduate of the Defense Systems Management College and a 1998 graduate of the Air War College.

The Dilemma

America's national military strategy relies on technologically superior forces to achieve its objectives when the military is called on to protect the nation and its interests. The common strategy is to protect this technology from potential adversaries and competitors. Competing with this need to maintain technological superiority is the need to preserve our defense industrial base, which has been reduced and consolidated due to military downsizing and the decreased demand for military goods. Without sufficient demand for their products, many defense contractors cannot remain in business. "Free market" forces will not save them, because technologies that are exclusive to military use cannot remain viable if there is no market.[1]

One procedure being used to maintain that technology and industrial base is to encourage the sale of US military goods to other countries as a means to expand the market for US military goods. The perceived need to sell overseas and the need to safeguard technology are often at opposing ends of the debate. In the post-cold-war era, there has been a concern that the current policies and strategies regarding exports are obsolete and need overhauling.[2] Coincidentally, the call for reexamining the policies is being championed alternately by those who want export controls and policies relaxed and those who believe we may already be transferring too much sensitive technology to potential adversaries. The question at the heart of the dilemma is this: Can the United States maintain a technologically superior force while it expands the defense industrial base beyond the needs of our military?

The debate will only become more heated in the twenty-first century. According to the Defense Intelligence Agency (DIA), competition for access or control of resources, markets, and technologies among major and regional powers beyond the year 2010 will increase.[3] The overall threat to US interests will be complicated by the proliferation of advanced technologies. The DIA acknowledges that key trends in military technology have the potential to change the nature of warfare and the characteristics of that threat.

Proliferation of advanced technology will have an impact on the US economic competitive position as well as the level of military threats to our security. Indicators monitored by the National Science Foundation show that the United States can expect competition for global market shares to escalate. Asia, not just Japan, is expanding as a trading partner and competitor with the United States.[4] The US technological lead in many areas, both civilian and military, will not remain secure in the twenty-first century.

While US and Western militaries are seen to have the edge in integrating various technologies, the greatest challenge may come from rogue nations or a subnational group possessing a critical system or technology that provides an asymmetrical edge or negates our advantage.[5] This paper examines the debate regarding whether and how to change current export controls and policies, discusses the current policies with an emphasis on how they relate to the defense industry, and concludes by looking at the strategic challenges facing the United States on technology transfer. Our strategy to deal with this world has changed, but not in a revolutionary fashion. At this point, we must look at how the strategy has evolved from our cold war mind-set.

How the United States Got Here

The US national security strategy goals broadly outline the role of technological advances and transfer of technology to other friendly nations. Those goals include bolstering America's economic prosperity and enhancing our security through the export of high-technology goods. To this end, the United States has been largely successful. The president proclaims the United States as a leading exporter in aviation, semiconductors, and software.[6] Yet, at the same time, the strategy acknowledges the existence of dangers in the technology revolution. More particularly, these dangers include "reverse engineering" and licensed production of US goods. In preparing for the twenty-first century, America must confront the reality that other countries could use US technology against the United States.

US national security strategy seeks to retain our superior technological and military capabilities.[7] To do this, administrations past and present have sought to limit access to sensitive equipment and technologies. Balancing this need with overall economic and national political goals is a delicate, but necessary, task.

During the cold war, the Coordinating Committee for Multilateral Export Controls (COCOM) was the main vehicle to limit technology transfer to communist countries. Established in 1947 COCOM operated on a consensus basis with all members of the North Atlantic Treaty Organization (NATO) (minus Iceland), Japan, and Australia.[8] While not perfect, it did limit technology transfer to potential adversaries in the Communist bloc. When communism fell, more markets opened and Western technology exports accelerated. COCOM had lost its basic function with telecommunications exports and the blurring of potential adversaries.[9] The world was no longer viewed as "East versus West." With proposals forwarded by representatives of the Clinton administration, the charter members agreed to disband COCOM in 1994 and replace it with another export control organization. Will this new organization protect US technology the same way that COCOM did? Is it realistic to believe that it can?

The New Forum

The current administration's strategy seeks to develop a replacement regime based on the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies of 1995.[10] This new regime will broadly focus on conventional weapons exports and sensitive dual-use technologies.[11] The founding nations have held numerous meetings since 1995. However, the United States did not publish an updated Department of Commerce Commodity Control List to reflect the Wassenaar Arrangement control list until January 1998, even though the WA was inaugurated in July 1996 so that the control lists would be effective in November 1996.[12] The development of this regime has been slow and is not com-

plete despite ever-increasing exports of sensitive and possibly dangerous technologies.

The Wassenaar Arrangement, initially known as the New Forum, has four separate elements or groups. Each group is assigned various functions to develop guidelines and administration and a secretariat to run the overall New Forum administration and the exchange of data submitted by members. The WA control lists, which include an extensive array of critical military technologies and goods, would seem to offer an excellent control mechanism for such items. But unlike COCOM, in which other nations had "veto power" over the export of a system or even the ability to evaluate a licensing application before its internal approval, the WA operates on "national discretion."[13] Vesting each nation with sole responsibility for determining the exportability of a particular system or technology creates many problems. Therefore, the United States should not deceive itself into believing that the New Forum is a one-for-one replacement for COCOM and that it will automatically provide protection of leading technologies. Other nations have the same concerns.

For example, the approval of many exports is subject to economic consideration as much as national security implications. In fact, member nations have continually accused the United States of putting economic interests first in exporting computers. In other examples of potential conflict, the United States has been concerned with the transfer of machine tools and data encryption.[14] Left unresolved, these and other areas of contention could undermine the arrangement and jeopardize the WA even before it is fully implemented.

The current US administration strategy also states that the United States is working to harmonize national export control policies with international forums and agreements. Additionally, the United States is committed to engagement with other militaries to build coalitions. Tools used in this engagement strategy include FMS and International Military Education and Training (IMET).[15] Coincidentally, one of the chief means of strengthening those relationships is selling modern weapons compatible with US systems. This procedure enhances interoperability and stand-

ardization with allies, allows formation of workable coalitions in case of future conflicts, and maintains a good working relationship through military-to-military communication.[16] However, the US national security strategy objective of strengthening ties with other militaries makes it difficult to harmonize internal export policies and international forums. Moreover, a strategy of technological superiority is unilateral, yet both the national security strategy and national military strategy assume the United States will fight within a coalition—and that requires interoperability and standardization. How significant is this paradox?

Technology and National Strategy

Overall, US national security strategy relies heavily on superior technology to offset decreases in military force structure due to downsizing. In short, we expect our quality to offset an adversary's quantity. Put another way, we prefer to pit firepower against manpower, much the same strategy we used during the cold war. The national security strategy seeks to maintain technological superiority of US forces by selectively increasing the modernization funding in some areas to field new systems as they reach the end of their service life. This heavy reliance on technologies is woven throughout the documents that outline the national military strategy.

In *Joint Vision 2010* the operational concepts underline that technologically superior equipment is essential to our military success.[17] The chairman of the Joint Chiefs of Staff acknowledges that many potential adversaries also possess modern technology.[18] The United States expects technology to offset smaller forces in the deterrence or prosecution of any future conflict. This assumption is a cornerstone of our strategy for the US military as we approach the twenty-first century.

This strategy is not new, however. Indeed, it is much the same as the long-standing strategy the United States had during the cold war: the United States expected numerical superiority enjoyed by the Warsaw Pact to be offset by United States and allied technological superiority. This same approach is seen as viable in the post-cold-war era.

Instead of large force-on-force numbers, the US military will rely on new technologies and concepts to win any future conflict.[19] Nonetheless, this advantage of technologically superior US military capabilities to establish national directives is not without complications and drawbacks.

One complication arises from the need to include allies and coalitions into future military planning. In this case, one of the main strategies is sharing US technology with these allies. For example, allies as well as our Air Force, Navy, and Marines Corps can purchase such new weapons systems as the Joint Strike Fighter (JSF).[20] With a planned first delivery by fiscal year 2008, the JSF is one of the first major weapons systems being designed for completion in the twenty-first century. Its development will represent leading-edge technology. Another concern is in the information arena, where the Defense Intelligence Agency (DIA) estimates that increased foreign military space capabilities will erode the relative advantage the United States has in satellite communications, surveillance, and navigation over the next decade.[21] Recent concerns regarding satellite technology transfer to China and its possible military use have made this DIA estimate even more timely.[22]

An additional challenge highlights the need to maintain a viable defense industrial base in light of downsized US military procurement. From 1985 to 1997 US defense procurement decreased by more than 60 percent.[23] In terms of lost experience, an estimated 2.5 million defense workers have been laid off from the beginning of the defense drawdown.[24] A viable, robust defense industrial base provides a means to procure the technologically superior weapons America needs to control unit costs. This article will show that maintaining industrial base, controlling costs, and protecting technology are independent but interrelated factors.

The Stakes

In the post-cold-war environment, US military strategy hinges on fielding superior operational capability while reducing the life-cycle costs of the weapon.[25] To manage the US defense industrial base to maintain its viability, the

United States must strike a delicate balance between downward budget pressures and obtaining the technologically superior weapons it needs at an affordable cost. In an unconstrained market, costs would be lowered by higher unit production, but US military requirements are decreasing. In addition, technology transfer from the United States could be strictly controlled (i.e., very limited) if that is indeed the only consideration. If unit costs were not a factor, the industrial base could be maintained more easily by simply keeping the production line open, but near idle. However, unit costs *are* a factor, so this is not a viable option. A systematic, strategic approach is required to balance the declining defense budget, the defense industrial base, and the role of FMS in supporting that industrial base.

US Defense Industrial Base

With US military downsizing, the US defense industry looks to foreign military sales and direct commercial sales (DCS)[26] as an important means to stay in business. As the military budget shrinks, the only way to lower the unit costs of newly acquired systems is to amortize the setup and development costs over a proportionally larger number of units. Just as the cost of the first 20 television sets would have been astronomical if they had been the only ones produced, the costs associated with producing 20 B-2 bombers are prohibitive by most measures in the post-cold-war era. The problem then is how to maintain an industrial base capable of sustaining a technologically superior military.

Declining Defense Budget

There is no foreseeable relief in the constrained size of the defense budget. Over the past 10 years, the Air Force budget authority for procurement has declined an average of 9.1 percent each year.[27] While the security threat remains uncertain in a multipolar world, the defense-spending trend continues its downward spiral. According to Dr. Paul Kaminski, former undersecretary of defense for acquisition and technology, the US defense industrial sector will

decrease another 10 percent (in dollars) before bottoming out in the next few years.[28] Clearly, US military requirements alone will not generate enough production to sustain America's aerospace industrial base.

The Use of Foreign Military Sales

To reach the goals of cost-effective weapons systems, the United States is looking toward FMS and DCS. The United States has three well-grounded reasons for seeking cooperative arms efforts with its allies.[29] First, these programs will help to strengthen military and industrial relationships that bring nations together. Second, any future conflict will most likely involve coalition forces that require interoperable equipment and logistics needs. Third, FMS will allow the United States to maintain its industrial base. According to Dr. Kaminski, "What we cannot afford individually may be affordable with a common effort."[30] Finally, there is the challenge of keeping production lines open. US defense contractors have depended on a consistent size and frequency of US military procurement to survive. With the number and frequency of these purchases diminishing, these contractors must look to modification work and international sales to survive; without it many companies would fail.

Dual-use technologies offer a unique set of opportunities and problems. The Defense Department is increasingly dependent on commercial and dual-use technologies, products, and processes. Because technological advances are increasing rapidly, the commercial sector is ahead of pure military applications in many areas, including electronics, computers, information processing, and communications.[31] Developing the technology in a laboratory is not the sole concern. In a technology-rich environment, future military success will gravitate towards the nation that capitalizes on commercial as well as military technology and rapidly incorporates advances into fielded weapons systems.[32] The speed with which a nation can integrate such advances may be the critical element in deterring conflict or, failing that, achieving victory.

What is at stake as America copes with this aspect of the post-cold-war environment is how to maintain a viable defense industrial base while not transferring technology that could be used against the United States or could negate a technological advantage. While a cooperative strategy in designing and procuring weapons systems has clear advantages, the loss of a bipolar world has complicated the ability of the United States to employ existing safeguards against unintentional transfer of sensitive technology. In turn this situation has rendered obsolete many assumptions regarding technology control.

Given that outcome, we must ask, are current safeguards enough to protect US technology and interests? I believe the answer is no, and a review of the present controls and some problems presented by the multipolar world provides an idea of the strategic course the United States needs to pursue.

Conflicting Policy Objectives

Revealing or uncovering controlled military information is called disclosure.[33] Information disclosure can occur through various means, including licensed production (sometimes called coproduction), cooperative research and development (R&D), discussions, visits, professional meetings and technical publications, and DCS or FMS.[34] For this context, our focus will be DCS, FMS, and coproduction.

Items determined to have a military application fall into two categories. The State Department licenses munitions items, the first category, for release. The second category includes dual-use items that have both commercial and military applications. The Commerce Department manages these items under its Control List, which falls under the Export Administration Act. While both categories have similar functions, they are governed by different regulations. The State and Commerce Departments approach the question of releasability (disclosure) for these categories with different mind-sets.

The primary authority governing the State Department's release of technology is the Arms Export Control Act (AECA), as amended. The AECA directs the State Depart-

ment to use export controls primarily to protect US national interests. The State Department also applies the International Traffic in Arms Regulations (ITAR) and establishes the munitions list with Defense Department concurrence. This authority protects the US military technological advantage and can be exercised without consideration of economic or commercial interests.[35] Within the changing world environment, technology transfer has also assumed increased importance as a political instrument. Therefore, the State Department sees FMS as a foreign policy tool instead of viewing it primarily as an economic tool.[36]

In contrast to the national security focus of the State and Defense Departments, the Commerce Department weighs primarily economic and trade considerations along with national security concerns in determining whether to release products and technology to international customers. It uses the Export Administration Act to control the export of dual-use items. While Commerce Department controls are also designed to protect national security, they are targeted at controlling exports to specific countries, including China, instead of broadly controlling a particular technology to export.[37] The differing decision-making strategies of the State and Defense Departments as opposed to the Commerce Department create uncertainty regarding the consistency of decisions. They also highlight the importance of whether an item is "dual-use" (as determined by the Commerce Department) or "military" (as determined by State with Defense concurrence).[38] Occasionally, the State Department will have jurisdiction over particularly sensitive technologies that Commerce considers dual-use. However, the influence of the State Department in this regard may be decreasing. Control by the Commerce Department over aircraft engine hot sections (critical to high-performance aircraft) and communications satellites are recent examples where control of technologies with a clear military application was taken from the State and Defense Departments and handled by the Commerce Department.

Export control of dual-use items has been a matter of jurisdictional contention between the State Department and the Commerce Department for years. As the defense

technology base declines, the resistance by some in industry to State Department control (that is, limiting dissemination) of dual-use technologies is mounting.[39] Additionally, some problems have occurred in highly sensitive technology transfers because of these unclear jurisdiction and interagency control issues. The Commerce and Defense Departments have disagreed over dual-use items as well.

One of the most sensitive and critical technologies the Air Force will rely upon in the twenty-first century will be superiority in radar-evading stealth technology. Just as importantly, the US military relies on enemy forces lacking the stealth technology that would negate our advantage. Stealth designs incorporate shapes, structures, materials, and processes that counter an enemy's ability to detect and locate US combat aircraft. The US lead in stealth technology is a critical element in our policy to offset quantity with smaller, more capable forces. The Government Accounting Office (GAO) reported in May 1995 that "lax export controls and unclear jurisdiction at federal agencies may put sensitive stealth technology into the hands of foreign governments, enabling them to build weapons capable of evading detection by US radar systems."[40] This report highlights the danger of differing positions and intent concerning technology transfer and national security. The GAO found that the Commerce Department's rules for referral of applications requests to other agencies did not require *either* State or Defense review on several key categories of stealth technology.

In essence, different criteria and lists increase the possibility for mistakes in technology transfer. By not mandating Defense involvement in the review process, the relationship between technology and national security may go unrecognized, possibly compromising US stealth advantages. This problem is not a new one, and evidence suggests it is getting worse.

The recent concerns over the export of missile and other technologies to China have also pointed to possible flaws in the current system. The problem of economic considerations in conflict with national security concerns is evident in the Loral-China connection. While Congress and others are investigating, the United States must ask if the com-

mercial strategy of opening foreign markets to high-technology goods has been overshadowed by the specter of creating national threats. Many analysts, within as well as outside the government, are reported to believe it has.[41] The problem is not a simple question of whether that technology given to China's satellite program could have a dual use. The question to be asked is this: Could unforeseen proliferation, within China and from China to a third country, lead to damage to US security interests that could be prevented? Reports claim that the May 1998 nuclear detonations in Pakistan were accomplished with assistance from China.[42] Out of concern for US national security, the House of Representatives quickly voted to ban further satellite technology transfers to China, for fear that such technology could find its way to Pakistan, one of China's customers for military hardware.[43]

The issue is complicated by the fact that much of what transferred is dual use. The control over satellite technology was taken from the State Department and given to the Commerce Department in December 1995 by executive order.[44] The Central Intelligence Agency reports that the technology is similar to that used in satellite launches and ballistic missiles.[45] With the technology being the same for military and commercial uses, the overall strategy needs to be centralized. Can the current safeguards be adjusted to fix it?

Inside the Defense Department, the Defense Technology Security Agency (DTSA) handles export policy. For the past several years, DTSA has been working with the State, Commerce, and Defense Departments to strike a balance between national security and the economic needs of the nation's defense industry to export.[46] DTSA reviews the export application (received from either from State or Commerce) and forwards it to the affected service(s) and the intelligence community for review. For many items, such as electronic warfare items, the vast array of foreign policy concerns and system capabilities makes it impossible to implement a uniform export control policy.[47] Case-by-case decisions on export releasability vary according to countries and systems, making the review process complex and, at the same time, subject to error. Additionally, in-

dustry has been pressing DTSA for relief from restrictions that some companies believe are too proscriptive.[48]

Within the Commerce, State, and Defense Departments there are a mosaic of rules, guidelines, objectives, and perspectives. To a defense industry trying to compete in a tough international marketplace, the array of export bodies and regulations can be confusing and time consuming. With two regimes (munitions items controlled by the State Department and dual-use items controlled by the Commerce Department), exporters must determine under which list their export item falls. When there is confusion, the exporter can ask State or Commerce to determine commodity jurisdiction. Since State controls are generally more restrictive than Commerce controls, an exporter could apply to Commerce to obtain license approval.

In summary, the competing views of the Commerce, Defense, and State Departments have created a possible vacuum in US policy dealing with technology transfer and national security. This view is not to suggest that the departments are not concerned with national security issues, only that they have differing views and perspectives. The main purpose of the Commerce Department is expanding and promoting trade. The State Department has experienced pressures both for and against the transfer of technology as a political tool. The Defense Department is more concerned with limiting technology transfer that could upset the United States' qualitative advantage on future battlefields. While all three departments have important roles to play, they often work at cross-purposes. The different control systems are complex, but complexity does not necessarily mean safer and greater effectiveness. As the complexity increases, the chances of a department accidentally exporting some process, technology, or system does not decrease. In fact, the chances of a department making a mistake frequently increase, and additional costs are involved. As the saying goes, in business, time is money. Complying with these complex sets of rules costs businesses time and money, particularly when a company does not know the appropriate controlling agency. Not only can this lack of knowledge be wasteful, it can cause a company to lose its all-important competitive edge.

Contradiction and Competition

As the United States exports military hardware, it may actually be building competition as well as selling products. That contradictory scenario causes competition between US firms and the foreign companies they create. The United States must weigh the benefits and drawbacks of its policy more fully. Pressures exist to expand the export market for the US defense industry. In June 1996, for example, Dr. Kaminski reported to a meeting of the NATO Workshop on Political-Military Decision-making in Warsaw, Poland, that someone needed to address the international environment for armaments cooperation. He stated that the Defense Science Board (DSB) has been tasked to help prepare the United States for the twenty-first century. The DSB will identify methods to ensure effective two-way access (between United States and its allies) to critical military technologies, methods to assure maximum use of commercial advances, and methods to develop a model for twenty-first-century armaments cooperation among allies. The challenge will enable the United States to create cooperation that preserves effective competition among industries in different countries.[49] This will be a difficult task.

Defense downsizing is widespread and is affecting markets worldwide. Indeed, competition among nations to sell arms in the global marketplace is creating a "buyer's market." Consequently, many nations with smaller technology bases are demanding a piece of the ever-decreasing defense industry pie. In their quest to carve out or preserve a military industry for their own country, these nations seek coproduction agreements with US contractors as an "offset" for doing business in their country. An offset is a form of industrial compensation a company offers for that country's defense-related purchase by either FMS or DCS. Coproduction is a specific type of offset where a portion of the weapons system is manufactured outside the United States. For aircraft manufacture, this may mean that the wings, portions of the engines, or certain avionics are manufactured, under license, in the foreign country. A major downside to this arrangement occurs when the FMS agreement merchandises not only the product but also the process by which the product is made. This procedure

allows the United States to lose some control over the weapons system manufacturing process.[50]

An example of coproduction is the ultimate US jet fighter for export, the F-16 Fighting Falcon. Designed as an export fighter and a mainstay for the US Air Force, the F-16 originally was coproduced in the United States and in NATO Europe. Later, as FMS was emphasized and expanded, the F-16 was coproduced in countries as diverse as Korea and Turkey. This type of technology transfer is becoming common and may be the wave of the future. Coproduction may encourage countries to invest in the American defense industry. However, a US firm clearly will benefit less when, for example, half of a fighter is built overseas, instead of having the entire aircraft manufactured in the United States. Concerns have surfaced recently over coproduction offsets. In 1996 the Commerce Department's undersecretary for export administration, William Reinsch, acknowledged a tentative effort by the United States to restrict the use of these types of offsets in international arms exports. In May 1996 Secretary Reinsch told a defense trade publication that growing demand in the Middle East and Asia for technology transfer could result in long-term problems for US industry by creating foreign competition.[51] The irony of offsets is that the technology transfer that makes many transactions possible today could put US companies at a distinct disadvantage tomorrow.[52]

A more insidious technology transfer involves software. As pressures to expand FMS continue, some foreign customers are demanding access to the software used to develop the system (source code) as well as the software used in the weapons system (object code) that traditionally has been supplied. When a foreign country receives source code as a form of technology transfer, it then possesses not only the product but the process as well. A foreign county needs a source code for many future changes in the aircraft capabilities and to correct discrepancies in its current operation. When a change to the aircraft software is required, the change is accomplished by using the source code in a development center called a software maintenance facility.[53] Once changes are made in the

source code, which engineers can read, it is translated into object code, which is used by the weapon system.

In response to increased demand for this capability, US policy may allow more aviation source code to be given to or sold to friendly nations.[54] In the case of aircraft avionics software, a country possessing the source code, maintenance facility, and trained personnel required to modify source code could incorporate changes without US approval or assistance. One software change could add weapons not intended by the United States, or even those not in the US inventory when the aircraft was sold to a foreign country. For example, the country could add an air-to-ship capability that was previously denied. Or, it could add an integrated electronic warfare system that could threaten US forces. The safeguards placed in the FMS process may or may not cover these unintended consequences, which could change the complexion of the sale. Another example: a defensive system could be given an offensive capability and range, and munitions loads could be enhanced. While safeguards remain in place, the shift in emphasis allowing source code sales inevitably permits a proliferation of software source code transfer.

In the face of these developments, the United States should not deceive itself by trusting the effectiveness of these safeguards. Hardware and software are difficult to keep secure in the first place. A recent purchase of supercomputers by nuclear weapons labs in the Commonwealth of Independent States (CIS) provides a painful reminder of how difficult it is to regulate technology transfer. When a balance between national security and economic commerce is attempted, the rules sometimes become confusing. Civilian customers (in CIS) can buy high-performance computers without going through the expensive licensing process. However, these customers cannot use these computers at a nuclear weapons facility without US government approval and a strict licensing review.

According to recent reports, the Commonwealth of Independent States apparently circumvented these guidelines and installed 16 IBM computers in the closed city of Arzamaz-16, where CIS had designed their hydrogen bomb. The United States is investigating the situation, but

Moscow has refused to allow investigators to interview any CIS witnesses, under the guise of national security. The administration relaxed these supercomputer export controls in 1995. However, anxiety over these recent sales—and a grand jury investigation into their legality—may spur a crackdown and greater scrutiny. This interest comes too late in this case. The IBM computers, along with computers sold earlier by Silicon Graphics under similar circumstances, have not been retrieved. Questions have surfaced regarding whether some of the computers are even located in the Commonwealth of Independent States.[55]

As alarming as this case is, some proponents of liberalized trade are fighting efforts to restrict exports of computer technology. According to Commerce Undersecretary Reinsch, the administration is not happy with proposed congressional actions, since they would include a 180-day review period. Such industry experts as John Scheibel, vice president and general counsel for the Computer and Communications Industries Association, fear the restrictions and 180-day review period would prove advantageous for US competitors.[56] Policy on release of the most sensitive source code is being studied on a case-by-case basis.[57]

Even with all the new emphasis on FMS, will it preserve the strength of the US industry base? Notwithstanding the implications of technology transfer, the current emphasis on FMS leaves open the question whether arms sales can help to preserve the defense industrial base.

FMS may not cure defense downsizing, but they loom large in the US defense industry's future. In 1993 FMS sales were a staggering $32.4 billion. Although foreign military sales have declined in the past three years, in 1996 they were $10.5 billion, making these sales a significant factor in US defense industry planning.[58] Nevertheless, even at that number, projected FMS will not offset the American and European cuts in defense acquisition spending.[59] The good news tells us that the projected sales will allow a more gradual decline, giving the United States some much-needed time to review its options.

Many officials in government and industry do not see a national security concern with increased sales of high-technology weaponry to foreign governments. For example,

sales of the F-4 and F-14 to Iran in the late 1970s are often cited as proof that safeguards are effective. Therefore, when the Shah was overthrown in 1979, Iran had state-of-the-art armament.

Here, the Achilles' heel of the Iranian Air Force (and what is held up as evidence that FMS safeguards worked) was Iranian dependence on the United States for spare parts and maintenance.[60] However, we should not totally rely on this lesson on how safeguards worked. Other countries have learned this lesson also. FMS and DCS agreements now include provisions for maintenance and spare parts, giving the FMS customer increased sustaining capability. In cases involving several F-16 FMS programs, where intrinsic depot capability is being added, dependence on continuous US support (and perhaps enhancements) is decreased even more dramatically. As foreign governments' dependence on US support decreases, so does US leverage.[61]

US industries are not the only areas of concern regarding technology transfer that have hurt our national security. Perhaps the most political concern was the Japanese and Norwegian sale of advanced milling machine equipment to the former Soviet Union in the 1980s. This equipment allowed the Soviets to build quieter nuclear submarines that were more difficult for the United States to detect.[62] Another, less publicized, case was the Dutch sale of night-vision equipment to Iraq just four months before Iraq's invasion of Kuwait.[63] International agreements and organizations can counter some of these sales, but the United States must start the countermovement by searching its own soul. America must continually ask itself if the short-term interest in selling high-technology arms to a foreign country can weaken our national security rather than strengthen it.

A Natural Conflict between Marketing and Security

In looking at any potential transfer of technology, we must keep in mind the objectives of the safeguards already in place. This observation comes as industry and many

government officials press for "reform" of such safeguards and policies. The debate is fierce, the stakes are high.

The cost of R&D resources required to field advanced technology weapons quickly could become cost-prohibitive. For example, the original plan to buy more than 100 B-2s made the more than $30 billion in R&D justifiable to officials at the Pentagon. In the post-cold-war era, the cost of the 21 B-2s actually manufactured make the case for those who say new weapons are too expensive. Spreading high-technology R&D costs over the production of numerically significant production lowers the overall unit production costs.[64] The B-2 unit cost more than quadrupled after the number to be purchased was cut, with some estimates showing the B-2 aircraft costing $2.2 billion a copy. The defense industry typically pushes overseas sales to gain economies of scale. Although no one is advocating selling B-2s abroad, we must consider candidates in other systems, subsystems, and technologies.

Nowhere is the debate more important than in the area of electronic warfare (EW). Many in the EW industry claim that US rules are placing US defense industries at a disadvantage in the world marketplace. Countries employing American EW systems want to have access to the software source code so they can make changes to their threat database without having to rely on the United States.[65] The across-the-board review of software release policies previously mentioned is being extended to EW software.[66]

In understanding the impact on national security, we should ask two questions. First, are US defense industries being blocked from competing with foreign countries? Second, if not blocked, what obstacles exist to inhibit US defense industries from competing in the international market? It appears the perception of the Department of Defense (DOD) regarding blocking arms sales is false. According to Dave Tarbell, director of the Defense Technology Security Agency, DOD rejected only 3 percent of the munitions cases and 9 percent of the dual-use cases it reviewed in 1994.[67] If this data is accurate, does industry have a basis for complaints?

According to some industry analysts, perhaps one problem lies with the US defense industry's culture since the

late 1940s. During the cold war, the US military provided a large, ready market for high-technology hardware and software. US industries came to depend on this stable market. This dependency has left US defense industries ill prepared to compete in the small-scale international market.[68] Even so, in the EW international marketplace, US firms control an estimated 70 percent of the market share.[69] This share results from the large number of US systems currently fielded by the United States and its allies and not based on the control policies in place.

The other problem lies in the maze of rules and the decentralized focus between the Commerce, Defense, and State Departments. As pointed out, the confusion that results can hinder US businesses and slow the review process, but it will not limit undesired technology transfer.

A Look to the Future

Many challenges are associated with the change from a bipolar to a multipolar world. The United States cannot define a single adversary, nor should it assume governments that are allies and "like governments" today will remain that way. Sometimes it is necessary to compete with one's allies and even cooperate with one's adversaries. National interests remain relatively constant, but allies come and go. As Germany and Japan illustrated earlier this century, allies can change places rather quickly.

Where the United States Is Today

Democratic reversals are not unknown in history. Examples include the overthrow of the liberal Italian government in the 1920s and the democratic Weimar Republic in Germany in the 1930s. The aborted coup attempt in the Soviet Union in August 1991 reminds us that the United States needs to protect its technological edge.[70] Many foreign customers of US firms need military assistance for the same reasons that make technology transfer a concern. These governments exist in an unstable environment.

With the demise of COCOM and rise of the Wassenaar Arrangement, attempts to reach international agreements

on technology transfer have become complex. The WA does not yield the same discipline or the control as did previous agreements. More players and thus more disagreements are present in the new environment. Since the new arrangement does not require any member country to honor another member country's denial to export a technology, there is no real control nor any way to circumvent denials. This arrangement makes it imperative that each member country coordinate and approve any move to deny technology transfers by the other countries. US attempts to implement a stronger policy have failed so far. Therefore, the United States cannot simply impose its will on the other members.

What the United States Needs to Do

What the United States needs to do falls broadly into two categories, domestic and international. Domestically, the United States needs to work towards a strong, central focus. The differing guidelines among State, Defense, and Commerce can confuse industry. Additionally, this system offers incentives for exporters to apply to the Commerce Department on items not controlled by the State Department and not reviewed by the Defense Department due to broader guidelines for approval. Therefore, the United States needs to pull back dual-use technologies under one organization. Because of the national security issues involved, I recommend this organization be an interagency group headed by the State Department. There are surely political as well as technical concerns involved in implementing this recommendation. I do not want to suggest that Commerce and Defense are not capable of implementing balanced controls over critical technologies. But the Commerce Department and the Defense Department each has its own philosophy; and none of the philosophies currently appears to hold an answer to where the ultimate responsibility should lie. Many of the rules that Commerce uses to limit distribution of technology are based on a bipolar world. The current bureaucracy with the dual-use items controlled by the Commerce Department may well be our Achilles' heel.

Controlling items simply by initial destination is not effective in a post-cold-war environment. International trade today means that once a technology leaves the country, the United States has limited control over its destination or use. We may attempt to impose restrictions on the sale of exported items to third countries, but we have had little success when it comes to processes and subcomponents. There is little we can do to enforce our intentions once the technology has left our hands. Licensing decisions made on narrow evaluation factors have a great potential for being shortsighted. The State Department adds its own bias to the process. If it becomes exceedingly difficult to have the State Department head up this effort, then another alternative would be for a separate forum of decision-makers from different agencies to resolve contentious issues and oversee the process. In any event, interagency cooperation must be strengthened to ensure a balanced focus, with national security as a paramount consideration.

The United States cannot take the same strategy used in the cold war and apply it to today's environment. Because of the number of licenses and the level of effort, the overall strategy needs a fresh look. Defense industry participation is crucial, but the US strategy cannot be based solely on economic issues. In many cases technology transfer agreements are conditions of the sale. In aerospace/defense, the vast majority of offset agreements require technology transfer, often as much as 50 percent or more of the offset.[71]

Clearly, there are political hurdles to overcome in developing a centralized control under the supervision of the State Department, but we need to work in that direction. The Defense Department, and specifically DTSA, needs a larger role in the review process of FMS, DCS, and dual-use sales.

Better interagency cooperation using today's structure is a good first step, but should the United States stop there? According to Dave Tarbell, director of DTSA, the United States must continue to have a disciplined export control process, and legislation must maintain the flexibility of the Executive Branch in dealing with controls and limits based on the changing environment.[72] This is good,

but the United States must ask if the strategy has a serious flaw. According to an Executive Branch working group's initial report on "Issues and Policy in International Technology," the government does not "have a comprehensive understanding of the effects on US national interests" of technology transfer.[73] Industry participation in any new strategy is essential, but inherent dangers must be recognized. Industry will be concerned primarily with its business base. We should not expect industries to police themselves exclusively, for they cannot be the lone driving force in determining how technology transfer affects national security. There are some good reasons to permit certain technology transfers, and to deny others, both for our interests and the interests of our allies. Central control, with a strategic view, needs to be the long-term domestic goal.

Internationally, the United States needs to work with members of the WA to develop tighter controls and a means to police the agreements. The WA will not guarantee that technology transfer will not occur that is adverse to the United States and its allies, since each member country may have a different view of the relative importance of the technology. Therefore, the United States must develop a complete strategy to determine which technologies are worth protecting and work with the international community to harmonize various meanings regarding "very sensitive" technologies. While the development of various "lists" is important, it does not provide a solution to the problem. This is particularly true if member nations do not all view the lists with the same vigilance in their controls of technology.

The rapid pace of technology advances and the increasingly complicated world of dual-use technologies make it imperative that our technology transfer strategy continues to evolve. No country can maintain an edge in all technologies. The United States must identify those technologies most critical to maintaining its military edge and then maintain superiority in industries involved with those technologies.[74] This strategy will provide us with choke points to control the spread of technologies that can affect national security. To make those choke points viable, US strategy must include other members of the WA.

While one key will be whether Defense has a voice in controlling military arms and dual-use technologies, other pressures will be felt within the Defense Department. The secretary of defense has issued strong guidance on international armaments cooperation to achieve standardization among "possible" coalition partners and to leverage US resources through cost sharing and economies of scale in weapons systems programs.[75] A critical question is how much influence Defense holds over export controls.

A Final Word

The future involves more bilateral and multilateral armaments cooperation because partnerships will be essential. Fewer nations and companies can afford to stay in business or build expensive, but infrequently purchased, defense systems. US military downsizing also will mean an increased likelihood of joint or coalition operations as the budgets decrease and threats become varied in the multipolar environment.[76] Teaming, collaborations, mergers, and acquisitions are becoming increasingly common in aerospace defense.

The fact remains that the lack of a single, well-defined enemy in the post-cold-war era will make it difficult for the US government to justify large expenditures that influence the US defense industry. Clearly, free market forces alone will be insufficient to save the defense industrial base.[77] Foreign military sales will remain an important part of the overall US strategy.

The US government needs to shape the debate by looking at ways to define what technologies (military and dual use) we are willing to transfer and ensure that national security objectives are not given a back seat to economic expediency. We must strengthen our national security by seeking international agreements to regulate technology transfers and arms sales. Most of all, we must continually evaluate the environment and shape our strategy based on the future and not solely on past decisions. Modification of cold war methodologies may be insufficient or ineffective.

Is it time to streamline our internal labyrinth of controls and centralize oversight and policy responsibilities? Cen-

tral control under the State Department could be effective if direction from the Executive Branch addressed the issues brought out in this paper. This would be a major undertaking. But a central voice, providing "one-stop shopping" for allies and US industry alike for answers and policy guidance, would enhance our ability to control technology transfer to meet national objectives of economic and military security. The fact that a certain technology can be transferred does not suggest that it should be transferred.

Is the current technology review and export control system broken? The COCOM regime has ended, but the Wassenaar Arrangement does not provide a total replacement. In the void between the two, critical technologies can flow to potential competitors and adversaries. The United States cannot afford the road of inaction. The small cuts the United States suffers now could soon be a hemorrhage. Even when completely implemented, the Wassenaar Arrangement will not protect our technology edge. Peacetime vigilance in this area is a fundamental aspect of military preparedness. We can ill afford to export the means of our future defeat.

Notes

1. Dual-use technologies with both commercial and military applications are more survivable in a free market, but they create concerns over proliferation if sold to potential adversaries.

2. Dave Tarbell, "Export Control Policies," *The DISAM Journal*, Fall 1995, 13.

3. Lt Gen Patrick M. Hughes, USA, director, Defense Intelligence Agency, "A DIA Global Security Assessment," *The DISAM Journal*, Summer 1997, 91.

4. Frank H. T. Rhodes, *Science and Engineering Indicators, 1996* (Washington, D.C.: National Science Board, Government Printing Office, 1996), 6–30.

5. Hughes, 97.

6. Executive Office of the President, *A National Security Strategy for a New Century* (Washington, D.C.: The White House, May 1997), ii.

7. Ibid., 1.

8. Richard F. Grimmett, "Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement," Congressional Research Service, 23 April 1996, 1.

9. Ibid., 2.

10. Executive Office, 8.

11. Grimmett, 3.

12. This information was provided by the Institute for Defense Analysis (IDA), Washington, D.C., in response to several questions posed by the author.

13. Norman D. Jorstad, director, Technology Identification and Analyses Center, "Multinational Activities to Establish the Wassenaar Arrangement on Export Controls," *Institute for Defense Analysis* 1 (March 1997): II-28–29.

14. IDA.

15. Jorstad, 17.

16. Paul G. Kaminski, undersecretary of Defense for Acquisition and Technology, "The FY 1997 DOD Acquisition and Technology Program," *The DISAM Journal*, Summer 1996, 89.

17. *Joint Vision 2010* (Washington, D.C.: Joint Chiefs of Staff, May 1997), 11.

18. Ibid.

19. *Global Engagement: A Vision for the 21st Century Air Force* (Washington, D.C.: Headquarters USAF, 1997), 3.

20. *Air Force Issues Book, 1997* (Washington, D.C.: Government Printing Office [GPO], 1997), 62.

21. Hughes, 97.

22. Ronald Brownstein et al., "Red Scare?" *U.S. News & World Report*, 8 June 1998, 20.

23. William J. Del Grego, *The Diffusion of Military Technologies to Foreign Nations* (Maxwell AFB, Ala.: School of Advanced Airpower Studies, Air Command and Staff College, March 1996), 4.

24. Ibid., 3.

25. Kaminski, 80.

26. *Direct commercial sales* refers to commercial sales, under license, directly to a foreign country, without the US procurement community managing the program as a "middleman" between industry and the foreign government.

27. "Air Force Almanac 1997," *Air Force Magazine*, May 1997, 42.

28. Paul G. Kaminski, "US Perspective on Defense Industrial Base Trends," *The DISAM Journal*, Winter 1996/97, 96.

29. Kaminski, "Acquisition and Technology," 89.

30. Ibid., 89.

31. Kaminski, "US Perspective," 93.

32. Ibid.

33. Katherine V. Schinasi, *Defense Industry: Trends in DOD Spending, Industrial Productivity, and Competition*, GAO Report (Washington, D.C.: General Accounting Office, 31 January 1997), 20.

34. Ibid.

35. Ibid., 5.

36. The Clinton administration has reaffirmed foreign military sales (FMS) as a "legitimate instrument of US foreign policy," making it a tool in the State Department. See *The Management of Security Assistance*, 16th ed. (Wright-Patterson AFB, Ohio: Defense Institute of Security Assistance Management, April 1996), 30–31.

37. Schinasi, 13.

38. Ibid., 6.

39. Ibid., 18.

40. David E. Cooper, director, Acquisition Policy, Technology, and Competitiveness Issues, *Export Controls: Concerns Over Stealth-Related Exports*, GAO Report NSIAD-95-140 (Washington, D.C.: General Accounting Office, 10 May 1995).

41. Several months ago a US congressional committee began an investigation into the selling of sensitive rocketry data by the Loral Corporation to the Peoples Republic of China under a US government license. See Robert S. Greenberger, Jackie Calmes, and John Harwood, "Shaken New World," *The Wall Street Journal*, 29 May1998, 1; *Washington Post*, 25 June 1998; and *New York Times*, 18 September 1998.

42. Robert Keatley, "How the Subcontinent Got the Bomb," *The Wall Street Journal*, 29 May 1998, A13.

43. Greenberger, 1.

44. Brian Duffy and Thomas Ricks, "Probe of Loral Aid to China Casts Light on Clinton Policy," *The Wall Street Journal*, 29 May 1998, A16.

45. The Associated Press, "CIA: China's Launchers, Missiles Similar," *USA Today*, 22 May 1998, 1.

46. Kaminski, "Acquisition and Technology," 34.

47. Ibid., 36.

48. Zachary A. Lum, "Let the Walls Come Tumbling Down?" *Journal of Electronic Defense*, March 1995, 38.

49. Kaminski, "Acquisition and Technology," 95.

50. Del Grego, 32.

51. In 1994 more than 40 percent of FMS sales were offset obligations. The trend is up from 35 percent in 1993. See Theresa Hitchens, "U.S. Offset Initiative Leaves Allies Cold," *Defense News*, 3–9 June 1996, 33.

52. Grant T. Hammond, *Countertrade, Offsets and Barter in International Political Economy* (London: Pinter Publications, Ltd., 1990), 57.

53. The use of the term *maintenance facility* is misleading. The software doesn't wear out or require maintenance. The facility is used to "modify" and test the software before loading it on an aircraft.

54. R. Noel Longuemare, memorandum, subject: Guidelines on International Transfers on Software Documentation (including source code), 8 April 1997, 2.

55. Jeff Gerth and Michael R. Gordon, "Russian Nuclear Lab Evaded Rules to Get Computers," *New York Times*, 27 October 1997, 1.

56. Michael S. Lelyveld, "Computer Industry Wants Curbs Vetoed," *Journal of Commerce*, 28 October 1997, 3.

57. Lum, 34.

58. DSAA Comptroller, *Financial Policy Division Report*, 30 September 1996, 1.

59. James Miskel, "Domestic Industry and National Security," *Strategic Review*, Fall 1991, 23.

60. Del Grego, 25.

61. Lum, 36.

62. Miskel, 26.

63. Ibid.

64. Barry M. Blechman and Ivan Oelrich, "B-2 Stealth Bomber Costs in Perspective," *Strategic Review*, Winter 1996, 7–16.
65. Lum, 34.
66. Ibid.
67. Ibid., 38.
68. Ibid.
69. Ibid., 41.
70. Miskel, 24.
71. Hammond, 84–85.
72. Tarbell, 13.
73. Briefing, Meeting of the Committee for National Security Working Group on Issues and Policy in International Technology for the National Science and Technology Council, subject: "Progress Report Briefing, Phase 1," 28 April 1997.
74. Ibid., 26.
75. William S. Cohen, secretary of defense, "DOD International Armaments Cooperation Policy," *The DISAM Journal*, Spring 1997, 70.
76. Kaminski, "Perspective on Defense," 94–96.
77. Leighton, 36–37.

*U.S. GOVERNMENT PRINTING OFFICE:1998-734-174/80104